International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 7 Issue 7, July 2020

ISSN: 2394-4404

A Framework Based On Institutional Theory To Aid In Cyber Resiliency In County Governments Of Kenya

Philip Akech

Masters student in Information Security and Audit at Jaramogi University of Science and Technology, Kenya

Dr. Samuel Liyala

Chair of Department of Information Systems, Jaramogi University of Science and Technology, Kenya

Dr. Silvance Abeka

Dean, School of Informatics and Innovative Systems, Jaramogi University of Science and Technology, Kenya

Abstract: ***Cyber resiliency is the ability of a system to anticipate, withstand, recover and evolve when a cyberattack has occurred in an organization or institution. Poor IT habits still persist in institutions exposing them to cyberattacks as institutions are failing to enforce cybersecurity standards to adequately protect against threats. The increase in cyberattacks occurring in organization due to rapid changes in the technological environment has made organizations recognize the importance of resiliency as an enhancement to cyber security. institutions such as County governments which carry out their functions through computing infrastructure are highly predisposed to cyberattacks due to the vast amount of information it has about its citizens. This paper investigates the role of the county management and the county employees in enhancing cyber resiliency in the County of Kakamega, Kenya, as the case study. A total of 70 respondents in the county participated in the survey. The results corresponded to the institutional theory of how institutional culture is formed. This study is significant as it does show that the resiliency of an institution is dependent of all who are involved in the institution or organization.***

Keywords: Cyber resiliency, cyber attack, cyber security, institution

I. INTRODUCTION

The number of cyber-attacks against global governments and commercial enterprises continues to grow in frequency and severity Ponemon (2015) and this called for the creation of Global Cyber Alliance to confront, address and prevent malicious cyber activity. There have been highly publicized cyber-attacks CyberArk & Vason Bourne (2016) with data breaches of consumer and government organizations which goes to show how cyber-attack is the main bane of technology

Governments have taken cognizance of the fact that IT sector is central to a nation's security, economy and public health and safety with businesses and private citizens becoming increasingly dependent upon the sector's functions (Homeland Security, 2016). The American president issued an Executive order (EO) 13636 which directed NIST to work with stakeholders to develop a voluntary framework NIST (2016) and with the framework in place, their critical infrastructure would have fewer cyber risks thus be depended upon to work at optimum levels in case of any attack.

Prior research has suggested that the main rationale of governments using IT for governance, is that it reduces costs and delays in processing and delivering services, expand citizen's access to public sector information, increase transparency and public accountability and weaken authoritarian tendencies (Haque, 2002). With large quantity of public and confidential data being created on a daily basis as the governments goes about their businesses, the security of confidential data becomes a fundamental issue and it is the duty of the government to secure this information Salifu (2008) and prevent unauthorized access.

ISSN: 2394-4404

Cyber security incidents are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors (PWC, 2015) with 76% of the respondents in an American survey saying that they were more concerned with cyber security threats up from 59% the year before. With such concerns, management of cyber security becomes paramount with development of standards for good practice of information security (ISO/IEC 27002: 2013, 2005) relevant to all types organizations, government departments included, that aims to increase assurance that incidences of cybercrime can be minimized to manageable levels and to prevent adverse effects. The scope of the ISO standards is universally accepted with every organization trying its best to adhere to them.

Many researchers and security designers of information systems have ignored non-technical issues like culture, laws, and other social issues of the individuals using the systems and the environments where these systems run (Yngström, 1996; Kowalski, 1994) .The technical measures that have been put in place that have been highlighted by various frameworks have aided in making systems become harder to attack and has acted as a deterrence but it has not solved the security problem as human side of using IT systems increase risks and because of this, criminals have turned their attention to the end users who are the weakest link in the chain Mwakalinga (2011) with social engineering attacks being the *modus operandi*. This is an indication that end users play a key role in abetting the increase in cybercrime albeit not intentionally and thus they are key in ensuring cyber security can be attained.

With cyber-attacks growing increasingly frequent and complex, cyber security strategies are shifting: while prevention is still important, it is more about prevailing Ponemon (2015) as all organizations at one point or another is bound to suffer attacks. Resilience is gaining importance as a core concept for improving sustainable welfare safety of a society Wohlgemuth, (2014) and with governments being a major consumer of IT with a large user base being citizens of all walks of life, resilience seems to be the best undertaking to complement the best practices and the frameworks that are in place. According to Ponemon Institute (2015) it posits that cyber resilience is considered to maximize employee productivity with 75%, 66% and 74% of respondents in North America, Germany and United Kingdom respectively.

Homegrown cyber criminals in Kenya are becoming more skilled and targeted Kigen (2015) with attacks on the IFMIS (Integrated Financial Management Information System) systems being examples and financial gain being a motivator as argued by (Aseef, 2012). Cyber security incidents have raised awareness but poor IT security habits still persist in organizations (CyberArk & Vason Bourne, 2016) and institution.

The purpose of this research was to develop a model that would aid the County government to be cyber resilient in the face of an attack as cyberattacks are a matter of when and not if it occurs. This study would benefit County governments and institutions to incorporate their employees from the management level to the lower level be actively involved in cyber resiliency and not leave cyber resiliency solely as the responsibility of the IT department.

II. LITERATURE REVIEW

A. CYBER RESILIENCY

The idea of achieving 100% (one hundred percent) protection is not only a fallacy, but also leads to false sense of security that exposes businesses and institutions to serious risk (Jeniffer, 2013). All organizations at one point of another is bound to suffer cyberattacks and these attacks are growing increasingly frequent and complex Ponemon Institute (2015). As the number of assets and system vulnerabilities continue to grow exponentially, the cyber threats are constantly evolving and increasing at the same pace (Jeniffer, 2013). In lieu of the above, the traditional form of security which centers on predictability alone cannot suffice to ensure that an organization is secure at all times thus a paradigm shift is a necessity.

Resiliency being a concept that has been adopted from medicine and health science is often associated with ecological systems demonstrating tolerance to and respective recovery from disruptions, which is also extended to human-made environment (Zalewski, 2015). Resilience is gaining importance as a core concept for improving sustainable welfare of a society (Wohlgemuth, 2014). Cyber resiliency as described by Bodeau (2011) is the ability of a system, organization, mission, or business process to anticipate, withstand, recover from and adapt capabilities in the face of adversary conditions, stresses or attacks on the cyber resources it needs to function. The goals for resilience (anticipation, withstand, recovery and adaptation) have been highlighted in the above definition as the core to which resilience is centered upon. Cyber resilience is becoming increasingly recognized as a critical component of comprehensive cyber security practices (Jeniffer, 2013) and thus paramount in the success of an organization or an institution.

The core difference between traditional security and resilience is that the former focuses on a specific threat, whereas the latter attempts to address uncertainties (Chmutina, 2016). Resilience is characterized by a temporality that combines the present with the future, but also actively deals with insecurities of the past as posited by (Cavelty, 2014). Thus resiliency is all about contingencies as opposed to predictability that organizations and institutions had become accustomed to, which marks a significant change in the modus operandi of cyber security of organizations. Resilience offer a means of understanding society as a system that exists in a constantly shifting relationship with an unpredictable and radically changing environment Cavelty (2014) which underscores the point that one can never attain 100% (one hundred percent) protection.

Within organizations, resilience resides in both the individual and organizational response to turbulence and discontinuities and an organizational system is composed of a complex network of interrelated elements and subsystems that interact through nonlinear relationships to form an organizations unique identity (Burnard, 2011). According to the constitution of Kenya (Constitution of Kenya, 2010), it conceptualizes county government as a geographical unit of devolved government of Kenya which qualifies it to be an institution of governance thus fit in to the definition of an

organization as so defined above. As such, the concept of cyber resilience is applicable as the county government is shifting its operations online to ensure that all its citizens and the populace in general can get services within or out of the county.

B. MANAGEMENT ROLE

It is quite evident that without management's support and involvement, IT professionals cannot safeguard information resources (Soomro, 2016). In comparison to hackers and system failures, employees are a major cause of data breaches partly due to their ignorance (Yeniman, 2011). Socializing with supervisors and colleagues goes a long way in influencing an employees' information security behaviors (Dang-Pham, 2017). As suggested by Veiga (2017), the task of instilling or changing Information Security Culture belong to Senior or Executive leadership

Information security concerns are generally low in the absence of a major loss because of poor measures which informs perceptions of managers (Taylor, 2015). Managers view information security as technology oriented Taylor (2015) thus heavy spending on technological countermeasures which can create a false sense of security thus resulting in management's overconfidence in their level of protection of information security. Technological measures alone cannot protect organizational information security and thus they require a great amount of the end-users' efforts (Dang-Pham, 2017). Organizations that have neglected to focus on individuals fail to achieve success in their efforts according to previous studies (Safa, 2016).

Regulatory requirements influence the attitude and behaviors of managers towards information security Alkalbani (2016) and it is a key factor for the reinforcement of an organizational authority within its industry and aid in avoidance of security risks (Kim, 2013). Senior management play a critical role in influencing the Information security culture instilled through their protection norms that filter down to all levels of employees Veiga (2017) and ensures that the organization complies with applicable laws and regulations. Managerial practices regarding information technology are the driver of IT effectiveness Soomro (2016) and for organizations to receive legitimacy, they have to comply with regulations on information security (Alkalbani, 2016).

Coercive pressures from regulatory institutions can influence organization's innovation activity and can help specify its structure or strategic adoption Kim (2013) and force the commitment of senior management to adopt certain institutionalized rules and practices in complying with information security (Alkalbani, 2016). It is one of the board's responsibilities is to ensure that the organization complies with applicable laws and regulations Veiga (2017) and thus guide employees' behavior in implementation processes and technology safeguards when processing information to be in line with the regulatory requirements. For effective information security management, information security managers should adopt a more holistic approach to include better managerial practices Soomro (2016) as the responsibility of an organization complying with applicable laws and regulations falls on senior management who are motivated to comply with the requirements due to regulatory pressures Alkalbani (2016) and their commitment affects employees' behavior in complying with standards and policies.

C. POLICIES, STANDARDS AND FRAMEWORKS

The table below summarizes the challenges presented by the frameworks that address cyber resiliency

Title	Authors	Challenges
Cyber Resiliency Engineering Framework (CREF)	(Bodeau, 2011)	- Socio-technical aspects are not the its main focus - It is not widely known - It is mainly centered towards Engineering and architecture
CERT Resilience Management Model (CERT-RMM)	(Richard A. Caralli, 2010)	- It is not widely known - It is best used after one has dealt with Capability Maturity Model Integration (CMMI) - It is mainly an enterprise management model for operations - Does not have clear defined goals and objectives as they are generic

Table 1: Cyber resiliency frameworks and their challenges

D. CONCEPTUAL FRAMEWORK

The conceptual framework included the independent variables with them being County management with the attributes taken into account being technical staff availability, management awareness, resiliency plan, security policies and the other variable being County employees with their attributes being employee attitude, employee awareness, information security policies and information security awareness.

Independent variables

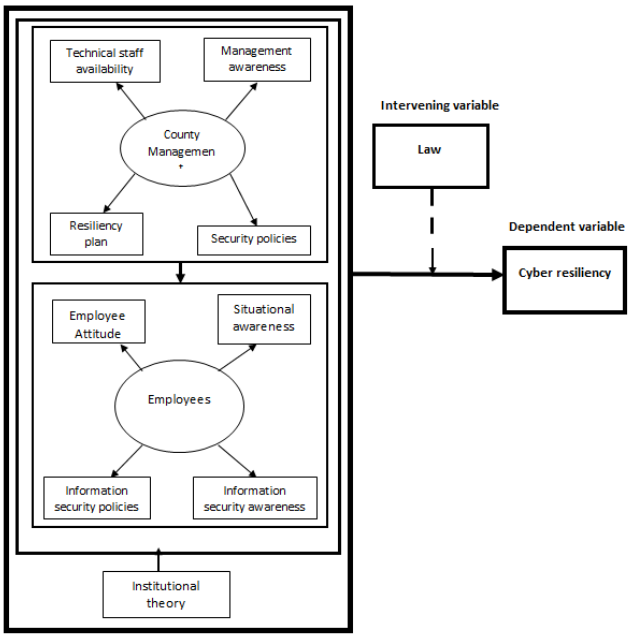

Figure 1: Conceptual Framework

III. RESEARCH METHODOLOGY

This study applied a quantitative research design which enabled the researcher to determine the relationship between independent variables and the dependent variable in the research. The population of the study was the employees and the management of the ten Ministries in the County Government of Kakamega in the Republic of Kenya. This study employed a random and purposive sampling technique for the selection of the samples to which 8 (eight) ministries took part in it. The selection involved staff who use computer infrastructure in their offices for their day to day operations in the Ministries that took part in the sampling.

This study employed the use of self-administered close-ended structured questionnaire due to its ability to collect data from respondents in a short period of time with confidentiality at its peak. A total number of 71 respondents constituted the sample size of the study having used the formula by deVaus (2002) to get the number of respondents

Face and content validity of the data collection instrument was ascertained by getting input from the supervisors and other experts in the Information Security field and thereafter iterative procedures of scale purification was applied. The composite reliability measures were above 0.8 which indicated the instrument's reliability and the values of average variance extracted was higher than 0.50 which showed adequate convergent and divergent validity using SmartPLS3 Ringle(2015) thus considered to be good and acceptable according to the convention.

IV. RESULTS

Responses from the questionnaires were summarized, edited, coded and allocated frequencies using the Likert scale responses ratings. Descriptive statistics was applied to determine the relationship among the collected data. The study found that 19% were Diploma holders, 61% were Degree holders and 20% were Masters holders with majority having between 0 – 2 years of experience.

Characteristics of respondents
Male 59% Females 41%
Experience 0 – 2 years 51% 3 – 4 years 29% 5 years 20%
Academic qualifications Diploma 19% Bachelors 61% Masters 20%

Table 2: Biodata of respondents

Measurement analysis was undertaken on the model using the SmartPLS3 with outer model loadings considered a form of item reliability for reflective models. According to Henseler (2012), the convention for a well-fitting reflective model, path loadings should be above .70 as shown in the table below

	CountyMgt	Employees	Law	Resiliency
Att2		**0.766**		
Att3		**0.819**		
MgtAwareness1	**0.791**			
MgtAwareness3	**0.764**			
Regulations1			**1.000**	
Resiliency				**0.891**
ResiliencyPlan1	**0.780**			
ResiliencyPlan2	**0.739**			
SituationAwareness1		**0.891**		
TechTeam1	**0.740**			
TechTeam1				**0.768**

Table 1: Factor loadings

From above factor loadings, the following statistics are summarized in the following tables

Path coefficients

	CountyMgt	Employees	Resiliency
Law	0.609	0.623	0.601

Table 2: Path coefficients

The path coefficients having been standardized does reflect strong paths

R square

	R Square	R Square adjusted
CountyMgt	0.371	0.358
Employees	0.388	0.375
Resiliency	0.361	0.348

Table 3: R square

According to Chin (1998) and Hock (2006)'s description of R square cutoffs, the results being above .33 shows they are moderate.

F square

	CountyMgt	Employees	Resiliency
Law	**0.590**	**0.635**	**0.565**

Table 4: F square

According to Cohen (1988), F square above .35 represents a high effect size and as per the above table, the effects are high.

Bootstrapping

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Law -> CountyMgt	0.609	0.622	0.076	8.015	0.000
Law -> Employees	0.623	0.637	0.101	6.141	0.000
Law -> Resiliency	0.601	0.604	0.094	6.389	0.000

Table 5: Bootstrapping

The t values above 1.96 are significant at the .05 level and which is the case in the above table meaning all paths are significant at better than the .001 probability level. This confirms that the F^2 is indeed effective and the path coefficients are indeed strong

Measurement fit

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
CountyMgt	**0.823**	**0.827**	**0.876**	**0.586**
Employees	**0.715**	**0.721**	**0.841**	**0.638**
Law	**0.600**	**0.603**	**0.833**	**0.714**
Resiliency	**0.565**	**0.617**	**0.816**	**0.691**

Table 6: Measurement Fit

Validated Model

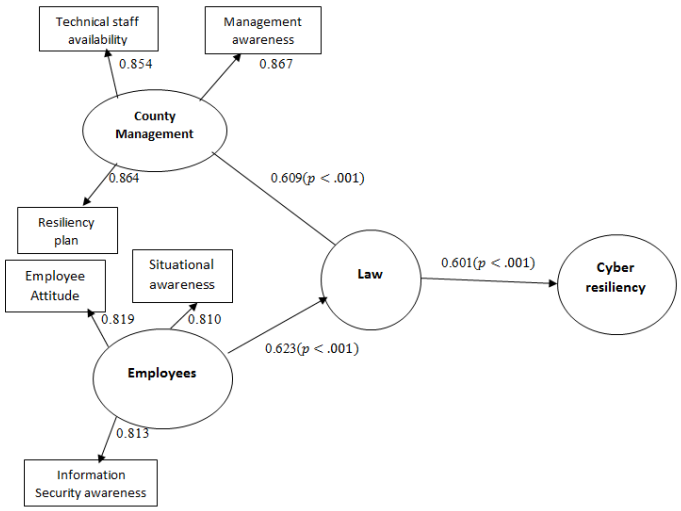

Figure 2: Validated model

V. DISCUSSION

From the findings, the path coefficients being closer to 1, shows that the effect is strong does go to show that law has a positive effect as a mediating factor on county management, employees and resiliency. The R square being above .33 does show that the effect of law as moderate but the F square being the change effect of R square shows that law has a larger effect on Employees, County management and resiliency respectively.

The findings of the bootstrapping show that the paths are significant at better than .001 probability level thus confirming the effect of law as a moderating factor is achieving resiliency as fundamental. The composite reliability being preferred to Cronbach's Alpha for PLS based research as the latter mostly underestimates the scale reliability, Chin (1998) and Hock (2006) suggest that composite reliability greater than .80 are good for confirmatory purposes, thus confirming that for resiliecy to succeed in Counties, the requisite laws have to be in place.

VI. CONCLUSION

The study revealed that for resiliency to succeed in an institution, law plays pivotal role in ensuring that the success of an institution is achieved. As resiliency is the new frontier in dealing with cybercrime as opposed to only prevention, the productivity of the employees increases as they feel better equipped to deal with cybercrime which are incessant in the technological environment.

VII. RECOMMENDATION

Having done the study in one County, 46 other Counties had not been factored in hence and overall picture of the Country cannot be inferred, thus the researcher suggests further studies to incorporate a sample of the counties to find the overall resiliency of the counties in the country and in extent, regional governments in a particular demography.

REFERENCES

[1] Adele da Veiga, N. M. (2017). Defining and Identifying the dominant information security cultures and subcultures. Computer & Security.
[2] Ahmed Alkalbani, H. D. (2016). Investigating the impact of institutional pressures on Information Security compliance in Organizations. Australian Conference on Information Systems. Wollongong: ACIS.
[3] Aseef, N. (2012). Cyber-Criminal Activity and Analysis.
[4] Constitution of Kenya. (2010).
[5] CyberArk & Vason Bourne. (2016). Global Advanced Threat Landscape Survey. Newton: CyberArk.
[6] Deborah J. Bodeau, R. G. (2011). Cyber Resiliency Engineering Framework. Bedford, MA: MITRE Corporation.
[7] Duy Dang-Pham, S. P. (2017). Investigation into the formation of information security influence: Network analysis of an emerging organization. Computer and Security, 111-123.
[8] Garson, G. D. (2016). Partial least Squares: Regression and & Structural Equation models. Asheboro: USA: Statistical Associates Publishing.
[9] Geuna Kim, S. K. (2013). What increases Firms' Performance of Information Security Management and the role of Regulatory Pressure. PACIS, (p. 100).
[10] Haque, M. S. (2002). E-governance in India: its impacts on relations among citizens, politicians and public servants. International Review of Administrative Sciences, Vol. 68, n.2: 231-20.
[11] Homeland Security. (2016, March 17). Retrieved from Homeland Security: www.dhs.gov/information-technology-sector
[12] ISO/IEC 27002: 2013. (2005). Information technology-Security techniques- Code of practice for information security controls. Geneve: International Organization for Standardization.
[13] Janusz Zalewski, S. D. (2015). Modeling Resiliency and Its Essential Components for Cyber physical Systems. Federated Conference on Computer Science and Information System, 107-114.
[14] Jeniffer Turgeon, E. D. (2013). Advancing Cyber Resilience Analysis with performance based Metrics from Infrastructure Assessments. International Journal of Secure Software Engineering, 75-96.
[15] Kevin Burnard, R. B. (2011). Organizational Resilience: Development of a conceptual framework for organizational response. International Journal of Production Research, 5581-5599.
[16] Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D.,... Shitanda, S. (2015). Kenya Cyber Security Report. Nairobi: Serianu.
[17] Ksenia Chmutina, G. L. (2016). Unpacking resilience policy discourse. Elseivier, 70-79.
[18] Mwakalinga, J. (2011). A framework for Adaptive Information Security Systems - A holistic Investigation.

[19] Myriam Dunn Cavelty, M. K. (2014). Resilence and (in) security: Practices, subjects, temporalities. Sage.
[20] Nader Sohrabi Safa, R. V. (2016). Information Security policy Compliance model in organizations. Computer & Security, 70-82.
[21] NIST. (2016, March 25). Retrieved from National Institute of Standards and Technology: http://www.nist.gov
[22] Ponemon. (2015). 2015 Cost of Cyber Crime Study: Global. Michigan: Ponemon Institute LLC.
[23] Ponemon Institute. (2015). The Cyber Resilient Organization: Learning to Thrive against Threats. Ponemon Institute.
[24] PWC. (2015). US cyber security: Progress Stalled. New York: Price Waterhouse Cooper.
[25] Richard A. Caralli, J. H. (2010). CERT Resilience Management Model. Hascom: Carnegie Mellon University.
[26] Richard G. Taylor, J. B. (2015). Perception deception: Security risks created by optimistic perceptions. Journal Of Systems and Information Technology, Vol 18 Iss 1: 2-17.
[27] Ringle, C. M. (2015). SmartPLS3. Boenningstedt: Germany: SmartPLS GmbH.
[28] Salifu, A. (2008). Impact of internet crime on development. Financial crime, Vol. 15 Iss:4,432-444.
[29] Waldo Rocha Flores, E. A. (2014). Information Security Knowledge sharing in organizations: investigation the effect of behavioral information security governance and national culture. Computers & Security, 90-110.
[30] Wohlgemuth, S. (2014). Resilience as a new Enforcement Model for IT. IEEE Security and Privacy Workshops. Darmstadt, Germany: Center for Advanced Security Research Darmstadt.
[31] Yeniman, Y. E. (2011). Factors influencing information security management in small and medium sized enterprises: a case study from turkey. International Journal of Information Management, 360-365.
[32] Zahoor Ahmed Soomro, M. H. (2016). Information security management needs more holistic approach. International Journal of Information Management, 215-225.